*DOCKET NO.: 3364P162*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

KOO-HONG KANG, ET AL.

Application No.:

Filed:

For: **In-Line Mode Network Intrusion Detect and Prevent System and Method Thereof**

Art Group:

Examiner:

Commissioner for Patents
P.O, Box 1450
Alexandria, VA 22313-1450

**REQUEST FOR PRIORITY**

Sir:

Applicant respectfully requests a convention priority for the above-captioned application, namely:

| COUNTRY | APPLICATION NUMBER | DATE OF FILING |
|---|---|---|
| Korea | 2003-0068718 | 2 October 2003 |

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP

Dated: 2/5/04

Eric S. Hyman, Reg. No. 30,139

12400 Wilshire Boulevard, 7th Floor
Los Angeles, CA 90025
Telephone: (310) 207-3800

# 대한민국특허청
# KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0068718
Application Number

출 원 년 월 일 : 2003년 10월 02일
Date of Application OCT 02, 2003

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Insi

2003 년 12 월 16 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2003.10.02

【발명의 명칭】 인 -라인 모드 네트워크 침입 탐지/차단 시스템 및 그 방법

【발명의 영문명칭】 IN-LINE MODE NETWORK INTRUSION DETECTION/PREVENTION SYSTEM AND METHOD THEREFOR

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【명칭】 유미특허법인

【대리인코드】 9-2001-100003-6

【지정된변리사】 이원일

【포괄위임등록번호】 2001-038431-4

【발명자】

【성명의 국문표기】 강구홍

【성명의 영문표기】 KANG,KOO HONG

【주민등록번호】 600503-1670815

【우편번호】 302-782

【주소】 대전광역시 서구 삼천동 국화한신아파트 602동 506호

【국적】 KR

【발명자】

【성명의 국문표기】 김익균

【성명의 영문표기】 KIM,IK KYUN

【주민등록번호】 680828-1690311

【우편번호】 305-721

【주소】 대전광역시 유성구 신성동 하나아파트 109동 1207호

【국적】 KR

【발명자】

【성명의 국문표기】 김병구

【성명의 영문표기】 KIM,BYOUNG KOO

【주민등록번호】 731109-1394918

【우편번호】 305-330
【주소】 대전광역시 유성구 지족동 열매마을아파트 1단지 107동 1404호
【국적】 KR
【발명자】
【성명의 국문표기】 이종국
【성명의 영문표기】 LEE,JONG KOOK
【주민등록번호】 740725-1797819
【우편번호】 305-350
【주소】 대전광역시 유성구 가정동 한국전자통신연구원 기숙사 2-302호
【국적】 KR
【발명자】
【성명의 국문표기】 김기영
【성명의 영문표기】 KIM,KI YOUNG
【주민등록번호】 660224-2551112
【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 122동 601호
【국적】 KR
【발명자】
【성명의 국문표기】 장종수
【성명의 영문표기】 JANG,JONG SOO
【주민등록번호】 611202-1670819
【우편번호】 305-761
【주소】 대전광역시 유성구 전민동 엑스포아파트 303동 903호
【국적】 KR
【심사청구】 청구
【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
유미특허법인 (인)
【수수료】

| | | | |
|---|---|---|---|
| 【기본출원료】 | 20 | 면 | 29,000 원 |
| 【가산출원료】 | 21 | 면 | 21,000 원 |
| 【우선권주장료】 | 0 | 건 | 0 원 |
| 【심사청구료】 | 12 | 항 | 493,000 원 |

【합계】 543,000 원
【감면사유】 정부출연연구기관
【감면후 수수료】 271,500 원
【기술이전】
【기술양도】 희망
【실시권 허여】 희망
【기술지도】 희망
【첨부서류】 1. 요약서·명세서(도면)_1통

# 【요약서】

## 【요약】

본 발명은 보호 네트워크와 외부 네트워크 사이에 연결되며, 보호 네트워크와 외부 네트워크 간의 침입 여부를 탐지하여 차단하는 인-라인 모드 시스템 및 그 방법에 관한 것이다.

본 발명에서는, 보호 및 외부 네트워크간에 상호 송수신하는 패킷을 모니터링하여 다양한 통계치 자료를 수집하며, 패킷 차단 규칙에 따른 패킷 필터링과 센싱 규칙에 따른 패킷 센싱을 수행하는 제1 네트워크 프로세서부와, 공격 시그너쳐를 기준으로 패킷의 페이로드(payload)를 조사하여 보호 또는 외부 네트워크로의 침입 여부를 검출하는 제2 네트워크 프로세서부를 포함한다.

또한, 본 발명은 검출한 침입 차단을 기가비트 이더넷 포트를 수용하여 실시간 처리함으로써, 네트워크 침입에 대한 빠른 대응을 할 수 있고, 기가비트급의 대용량 트래픽을 안정적으로 처리할 수 있다. 그리고, 트래픽을 미터링하는 규칙에서부터 필터링 규칙 및 센싱 규칙에 이르기까지 침입 여부를 검출 및 차단하는데 필요한 각종 기준들을 관리자를 통해 실시간으로 업데이트할 수 있도록 하며, 이를 통한 사용의 편리성 및 경제적 이점을 누릴 수 있도록 한다.

## 【대표도】

도 2

## 【색인어】

침입 탐지/차단, 네트워크 프로세서, 스노트 룰, 어기어사, APP500

【명세서】

【발명의 명칭】

인-라인 모드 네트워크 침입 탐지/차단 시스템 및 그 방법 {IN-LINE MODE NETWORK INTRUSION DETECTION/PREVENTION SYSTEM AND METHOD THEREFOR}

【도면의 간단한 설명】

도 1은 본 발명의 실시예에 따른 인-라인 모드 네트워크 침입 탐지/차단 시스템이 적용된 네트워크 구성을 도시한 도면이다.

도 2는 도 1에 도시한 인-라인 모드 네트워크 침입 탐지/차단 시스템의 대략적인 구성을 도시한 도면이다.

도 3은 도 2에 도시한 제1 네트워크 프로세서의 세부적인 구성을 도시한 도면이다.

도 4는 본 발명의 실시예에 따라 제2 네트워크 프로세서로 전달하는 패킷 데이터의 구성을 도시한 도면이다.

도 5는 도 2에 도시한 PL3 브리지 FPGA의 구성을 세부적으로 도시한 도면이다.

도 6은 도 2에 도시한 제2 네트워크 프로세서의 구성을 세부적으로 도시한 도면이다.

도 7은 도 2에 도시한 제2 네트워크 프로세서부의 동작 과정을 순차적으로 도시한 흐름도이다.

도 8은 도 7에 도시한 싱글 블록 처리 과정을 순차적으로 도시한 흐름도이다.

도 9는 본 발명의 실시예에 따른 싱글 블록 생성 과정을 개념적으로 도시한 도면이다.

도 10은 도 7에 도시한 시작 또는 중간 블록 처리 과정을 순차적으로 도시한 흐름도이다.

도 11은 본 발명의 실시예에 따른 시작 블록 또는 중간 블록 생성 과정을 개념적으로 도시한 도면이다.

도 12는 도 7에 도시한 마지막 블록 처리 과정을 순차적으로 도시한 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<13> 본 발명은 네트워크 침입 탐지/차단 시스템 및 그 방법에 관한 것으로서, 보다 상세하게는 네트워크상의 침입 또는 공격을 검출하여 차단시키는 인-라인(In-Line) 모드 시스템 및 그 방법에 관한 것이다.

<14> 근래 들어, 컴퓨터와 인터넷 사용의 대중화와 함께 네트워크에 대한 침입이나 공격 패턴 역시 빠른 속도로 진화하고 있으며, 이러한 공격들이 네트워크를 마비시킴으로서 전자 상거래 서비스 중단과 같은 심각한 경제적 손실에서부터 인터넷 서비스 중단에 따른 극심한 사회적 혼란을 초래한다.

<15> 이로 인해, 오늘날 네트워크 대역폭의 급속한 증가와 날로 지능화되어 가는 있는 해커(hacker)들의 공격에 대처하기 위한 침입 탐지 시스템(Intrusion Detection System, 이하 'IDS' 라 함)은 하드웨어 측면에서 뿐만 아니라, 소프트웨어 측면에서도 진일보된 변화된 구조를 가져야한 한다.

<16> 자세히 설명하면, 종래의 IDS는 호스트 IDS 제품과 네트워크 IDS 제품으로 구별된다.

<17> 먼저, 호스트 IDS 제품은 오디팅(auditing) 시스템이나 이벤트 로그(event logs)를 이용하여 서버 또는 개인용 컴퓨터와 같은 하나의 종단 시스템 또는 네트워크 애플리케이션(Application)을 보호한다.

<18> 반면, 네트워크 IDS 제품은 네트워크 트래픽을 모니터링하여 공격 또는 침입을 감지해 해커(hacker)들의 공격을 차단한다. 이러한 네트워크 IDS 제품은 오늘날 다음과 같은 세 가지 분야, 시그너쳐(signature) 검출, 에노멀리(Anomaly) 검출, 그리고 서비스 거부(Denial of Service) 검출과 같은 어느 하나의 분야에 집중해 개발되고 있다.

<19> 한편, 해커들은 이전에 성공적으로 사용된 공격 방법을 이용해 네트워크를 공격한다. 이러한 공격들은 네트워크 보안 제품 생산자들에 의해 분석되어지고, 이를 통해 자세한 프로파일(Profile) 또는 공격 시그너쳐가 만들어진다.

<20> 이러한 공격 시그너쳐 검출 기술은 네트워크 트래픽 내에 공격 지문(fingerprint)을 조사하고 이를 알려진 시그너쳐와 비교함으로서, 네트워크 공격 또는 침입을 검출해낸다. 이후, 이러한 공격 시그너쳐가 입력 트래픽 내에서 확인되면, 보안 시스템은 알람 또는 경보 신호를 발생하여 네트워크 관리자가 이를 인지할 수 있도록 한다.

<21> 오늘날 흔히 사용되는 방화벽(firewall)은 유입된 패킷을 차단/통과 여부를 결정하기 위해 패킷 헤드 내 IP 또는 포트 주소와 같은 특정 필드만을 검사한다. 이로 인해, 방화벽은 트래픽 내 시그너쳐를 검출하기에는 불가능하다.

<22> 반면, 스노트(Snort) 제품은 립캡(lipcap)을 이용하여 패킷 내 임의의 위치에 존재하는 시그너쳐를 검출해 내는 네트워크 IDS 제품이다.

<23> 그러나, 이러한 스노트 제품들은 순수 소프트웨어로 구현되어 있기 때문에, 오늘날과 같이 점점 빨라지고 있는 네트워크의 속도로 인해 증가된 네트워크 대역폭을 따라잡기에는 불가능하다.

<24> 즉, 스노트 제품들은 범용 프로세서의 기술 발전이나 메모리와 같은 서브 시스템 연결 측면에서 볼 때, 상기한 기가비트(Gigabit) 인터넷 인터페이스 속도를 따라가지는 못한다.

<25> 따라서, 더욱 증가된 대역폭을 감당하기 위해 ASIC(Application Specific Integrated Circuits : 주문형 반도체, 이하 'ASIC' 라 함) 형태의 전용 하드웨어 가속기를 사용하여 성능 향상을 시도하는 네트워크 IDS도 있다.

<26> 그러나, 이러한 시도는 성능 문제는 해결할 수 있으나, 프로토콜 변화나 다양하게 변화하는 공격의 유형에 적절하게 대응하기에는 어려움이 따른다. 즉, ASIC 개발 사이클이 빠르게 변화하는 네트워크 침입 환경에 적절히 대응하기에는 현실적으로 많은 어려움이 있다.

<27> 따라서, 빠르게 변화하는 네트워크 침입을 탐지할 수 있는 시스템 및 그 방안이 절실히 요구되고 있는 실정이다.

【발명이 이루고자 하는 기술적 과제】

<28> 본 발명이 이루고자 하는 기술적 과제는 이러한 문제점을 해결하기 위한 것으로서, 네트워크로의 침입 여부 확인 및 그에 따른 공격 차단을 기가비트 이더넷 포트를 수용하여 실시간으로 처리함으로써, 네트워크 침입에 대한 빠른 대응 및 기가비트급의 대용량 트래픽을 안정적으로 처리할 수 있는 인-라인 모드 네트워크 침입 탐지/차단 시스템 및 그 방법을 제공하기 위한 것이다.

<29> 또한, 본 발명은 트래픽을 미터링하는 규칙에서부터 필터링 규칙 및 센싱 규칙에 이르기까지 공격 여부를 검출하는데 필요한 각종 기준들을 관리자(개인용 컴퓨터)를 통해 실시간으로 업데이트할 수 있는 인-라인 모드 네트워크 침입 탐지/차단 시스템 및 그 방법을 제공하기 위한 것이다.

【발명의 구성 및 작용】

<30> 이러한 목적을 달성하기 위한 본 발명의 특징에 따른 인-라인 모드 네트워크 침입 탐지/차단 시스템은, 보호 네트워크와 외부 네트워크 사이에 연결되며, 상기 보호 네트워크와 상기 외부 네트워크 간의 침입 여부를 탐지하여 차단하는 시스템에 있어서, 외부로부터 수신하는 PDU(Packet Data Unit)를 모니터링하여 미터링 규칙에 따라 각종 통계치 자료를 수집하며, 상기 수신한 PDU를 패킷 차단 규칙에 따라 선택적으로 폐기하거나 통과시키고, 센싱 규칙에 따라 상기 수신한 PDU를 복사한 복사 PDU를 만드는 제1 네트워크 프로세서부; 상기 제1 네트워크 프로세서부로부터 수신하는 PDU의 페이로드(payload)에 대해 적어도 한 개 이상의 공격 시그너쳐를 이용하여 상기 보호 및 외부 네트워크간의 침입 여부를 탐지하는 제2 네트워크 프로세서부; 및 상기 제2 네트워크 프로세서부에서 탐지한 침입을 차단할 수 있는 규칙인 패킷 차단 규칙을 생성하거나 갱신하여 상기 제1 네트워크 프로세서부로 제공하는 개인용 컴퓨터를 포함한다.

<31> 그리고, 외부의 기가비트 이더넷 인터페이스(Gigabit Ethernet Interface)로부터 수신하는 적어도 한 개 이상의 PDU를 상기 제1 네트워크 프로세서부로 전달하는 라인 인터페이스부를 더 포함한다.

<32> 또한, 본 발명의 특징에 따른 인-라인 모드 네트워크 침입 탐지/차단 방법은, 보호 네트워크와 외부 네트워크 사이에 연결되며, 상기 보호 네트워크와 상기 외부 네트워크 간의 침입

여부를 탐지하여 차단하는 방법에 있어서, a)외부로부터 수신하는 PDU(Packet Data Unit)를 적어도 한 개 이상 폐기시키거나 그대로 통과시킬 수 있는 기준인 패킷 차단 규칙을 생성하는 단계; b)상기 생성한 패킷 차단 규칙에 따라 상기 수신하는 PDU를 선택적으로 폐기하거나 통과시키는 단계; 및 c)상기 통과시킨 PDU의 페이로드(payload)에 대해 적어도 한 개 이상의 공격 시그너쳐를 이용하여 상기 보호 및 외부 네트워크간의 침입 여부를 탐지하는 단계; 및 d)상기 탐지한 침입을 차단할 수 있는 규칙을 생성하거나 업데이트하여 상기 탐지한 공격을 차단시키는 단계를 포함한다.

<33> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였다. 명세서 전체를 통하여 유사한 부분에 대해서는 동일한 도면 부호를 붙였다.

<34> 도 1은 본 발명의 실시예에 따른 인-라인 모드 네트워크 침입 탐지/차단 시스템이 적용된 네트워크 구성을 도시한 도면이다.

<35> 도 1에 도시되어 있듯이, 본 발명의 실시예에 따른 인-라인 모드 네트워크 침입 탐지/차단 시스템(200)은 기가비트 이더넷 인터페이스(101, 102)를 통해 제1 및 제2 네트워크(110, 120)와 상호 연결된 구조를 이룬다.

<36> 이로 인해, 인-라인 모드 네트워크 침입 탐지/차단 시스템(200)은 제1 및 제2 네트워크(110, 120) 사이를 지나는 모든 패킷들에 대한 네트워크 공격 여부 검출 및 검출된 공격 차단을 수행한다.

<37> 여기서, 제1 네트워크(110)는 공격으로부터 보호할 보호 대상 네트워크이며, 제2 네트워크(120)는 외부 네트워크이다.

<38> 이처럼, 본 발명의 실시예에서는 보호할 대상 네트워크와 외부 네트워크로의 공격 여부 검출 및 검출된 공격 차단 등을 수행하는 것에 대해 설명하고자 하지만, 이는 본 발명에 한정되는 것이 아니라 경우에 따라서는 적어도 두 개 이상의 각 네트워크에 대한 공격 여부 검출 및 공격 차단 등을 수행할 수도 있다.

<39> 도 2는 도 1에 도시한 인-라인 모드 네트워크 침입 탐지/차단 시스템의 대략적인 구성을 도시한 도면이다.

<40> 도 2에 도시되어 있듯이, 인-라인 모드 네트워크 침입 탐지/차단 시스템(200)은 라인 인터페이스부(210)와 제1 네트워크 프로세서부(220), 제2 네트워크 프로세서부(230) 및 개인용 컴퓨터(240)를 포함한다.

<41> 라인 인터페이스부(210)는 제1 및 제2 기가비트 이더넷 포트(211, 212)와 기가비트 PHY 칩(213)을 포함하며, 제1 네트워크 프로세서부(220)는 제1 네트워크 프로세서(221)와 PL3 브리지 FPGA(Filed Programmable Gate Array, 이하 'FPGA' 라 함, 222)칩을 포함한다. 그리고, 제2 네트워크 프로세서부(230)는 제2 네트워크 프로세서(231)을 포함한다.

<42> 이때, 본 발명의 실시예에서는 제1 및 제2 네트워크 프로세서(221, 231)를 어기어(Agere)사에서 제공하는 5G 솔루션 APP500을 사용하는데, 이는 본 발명에 한정되는 것이 아니라, 경우에 따라서는 다른 회사에서 제공하는 다른 프로세서를 사용할 수도 있다.

<43> 먼저, 라인 인터페이스부(210)는 제1 및 제2 기가비트 이더넷 포트(211, 212)를 통해 외부의 기가비트 이더넷 인터페이스(101, 102)와 각각 접속한다.

<44> 제1 네트워크 프로세서부(220)는 인터넷 커뮤니티의 네트워크 관리 프로토콜에서 사용하는 IETF RFC 2863 인터페이스 그룹 MIB(Management Information Base)에 해당하는 통계치 자료와 제1 네트워크(또는 제2 네트워크)로부터 수신하는 모든 패킷에 대한 다양한 통계치 자료를 수집하는 트래픽 미터링(traffic metering)을 수행한다.

<45> 이와 동시에, 제1 네트워크 프로세서부(220)는 송신지 IP 주소와 목적지 IP 주소, 송신지 포트 주소, 목적지 포트 주소, 프로토콜 및 TCP 플래그 비트 중 적어도 어느 하나를 포함하거나, 또는 두 개 이상의 조합으로 이루어진 패킷 차단 규칙에 따라 패킷 필터링(filtering)을 수행한다.

<46> 또한, 이와 동시에 제1 네트워크 프로세서부(220)는 송신지 IP 주소와 목적지 IP 주소, 송신지 포트 주소, 목적지 포트 주소, 프로토콜 및 TCP 플래그 비트 중 적어도 어느 하나를 포함하거나, 또는 두 개 이상의 조합으로 이루어진 센싱 규칙에 따라 해당 패킷에 대한 센싱(sensing)을 수행한다.

<47> 다음으로, 제2 네트워크 프로세서부(230)는 스노트사에서 제공하는 공격 시그너쳐를 기준으로 제1 네트워크 프로세서부(220)로부터 수신하는 패킷의 페이로드(payload)를 실시간으로 조사하여 보호 또는 내부 네트워크(110, 120)로의 침입 여부를 탐지한다.

<48> 개인용 컴퓨터(240)는 검출한 공격을 차단하기 위한 규칙을 생성하거나 갱신하여 제1 네트워크 프로세서부(220)로 제공하며, 센싱 규칙 역시 관리자(administrator)의 요청 사항에 따라 새로 생성하거나 또는 갱신하여 제1 네트워크 프로세서부(220)로 제공한다.

<49> 이때, 개인용 컴퓨터(240)는 IDS 운영을 위해 필요한 다양한 애플리케이션을 구동한다.

<50> 이러한 구성을 갖는 인-라인 모드 네트워크 침입 탐지/차단 시스템(200)에서패킷 흐름 과정을 살펴보면, 먼저 두 개의 제1 및 제2 기가비트 이더넷 포트(211, 212)를 통해 외부로부터 이더넷 프레임(Ethernet frame)을 수신한다.

<51> 수신된 이더넷 프레임은 기가비트 PHY 칩(213)과 32비트 POS-PHY(Packet Over SONET-Physical Layer Protocol, 이하 'POS-PHY' 라 함) 레벨 3 인터페이스(201)를 통해 제1 네트워크 프로세서(APP500, 221)로 전달된다.

<52> 이후, 제1 네트워크 프로세서(221)에서 스위칭된 이더넷 프레임은 PL3 브리지 FPGA 칩(222)을 경유해 32 비트 POS-PHY 레벨 3 인터페이스(202)와 기가비트 PHY 칩(213)을 통해 제1 및 제2 기가비트 이더넷 포트(211, 212)로 출력된다.

<53> 즉, 제1 기가비트 이더넷 포트(211)로 수신되는 이더넷 프레임은 제1 네트워크 프로세서부(220)를 경유해 제2 기가비트 이더넷 포트 2(212)로 빠져나가는 반면, 제2 기가비트 이더넷 포트 2(212)로 수신되는 이더넷 프레임은 제1 네트워크 프로세서부(220)를 거쳐 제1 기가비트 이더넷 포트(211)로 빠져 나간다.

<54> 이를 통해, 제1 네트워크(110)와 제2 네트워크(120)는 논리적으로 상호 투명하게 연결되어 침입 탐지/차단 시스템(200)으로 하여금 인-라인 모드로 동작하게 한다.

<55> 도 3은 도 2에 도시한 제1 네트워크 프로세서(221)의 세부적인 구성을 도시한 도면이다.

<56> 도 3에 도시되어 있듯이, 제1 네트워크 프로세서(221)는 분류기(223)와 트래픽 매니저(traffic manager, 224), 스테이트 엔진(state engine, 225) 및 PCI 인터페이스(226)를 포함한다. 이때, 분류기(223)는 제1 패스(223a,)와 제2 패스(223b)를 포함하며, 트래픽 매니저(224)는 멀티캐스터(224a)와 패킷 변환 엔진(224b)을 포함한다.

<57> 자세히 설명하면, 분류기(223)는 개인용 컴퓨터(240)로부터 수신하는 미터링 규칙, 필터링 규칙, 그리고 센싱 규칙을 기준으로 입력 PDU(Packet Data Unit, 이하 'PDU' 라 함)와의 패턴 매칭(pattern matching)을 통해 외부로부터 수신하는 PDU를 분류하며, 트래픽 매니저(224)는 센싱 규칙에 의해 분류한 PDU에 대해 멀티캐스팅 및 패킷 변환을 수행한다.

<58> 그리고, 스테이트 엔진(225)은 외부로부터 수신하는 모든 패킷 데이터와 관련한 다양한 통계치 자료를 수집하며, PCI 인터페이스(226)는 PCI 버스(204)를 통해 개인용 컴퓨터(240)와의 데이터 송수신을 수행한다.

<59> 자세히 설명하면, 스테이트 엔진(225)이 수집하는 다양한 통계치에 대한 표시예가 [표 1]이다.

<60> [표 1]에 도시되어 있듯이, 스테이트 엔진(225)은 기본적인 통계 데이터를 실시간으로 수집하며, 수집한 통계 데이터는 PCI 인터페이스(226)를 통해 개인용 컴퓨터(240)로 전달한다.

<61> [표 1]

<62>

| 종류 | 이름 | 설명 |
|---|---|---|
| 인터페이스 통계치 | InInOctets | 수신 옥텟(octet) 수 |
| | InInUcastOkts | 목적 IP 주소가 클래스 A,B,C 타입의 수신 패킷 수 |
| | IfInDiscards | 내부수신 버퍼 고갈에 의해 폐기된 패킷 수 |
| | IfInErrors | 수신 패킷의 레어어 3 헤드 에러 |
| | IfInUnkownProtos | 지원되지 않거나 알 수 없는 레이어 3 프로토콜의 수신 패킷 수 |
| | IfOutOctets | 송신 옥텟 수 |
| | IfOutUcastPkts | 목적 IP 주소가 클래스 A,B,C 타입의 송신 패킷 수 |
| | IfOutDiscards | 송신 버퍼 고갈에 의해 폐기된 패킷 수 |
| | IfOutErrors | 송신상에 문제 발생된 패킷 수 |
| | IfInMulticastPkts | 목적 IP 주소가 클래스 D 타입의 수신 패킷 수 |
| | IfInBroadcastPkts | 목적 IP 주소가 브로드캐스트 주소인 수신 패킷 수 |
| | IfConnctorPresent | 링크 업/다운 |

<63> 그리고, 스테이트 엔진(225)은 개인용 컴퓨터(201)로부터 수신하는 트래픽 미터링 규칙에 따라 특정 트래픽의 통계치 데이터를 수집하는데, 이때 트래픽 미터링 규칙은 앞서 언급한

바와 같이 송신지 이더넷 주소, 목적지 이더넷 주소, 이더넷 타입, 송신지 IP 주소, 목적지 IP 주소, 송신지 포트 주소, 목적지 포트 주소, 프로토콜, TCP 플래그 비트 중 적어도 어느 하나를 포함하거나, 또는 적어도 두 개 이상의 조합으로 이루어진다.

<64> 다음으로, 분류기(220)는 두 개의 패스(Pass)로 입력된 PDU를 처리하는데, 제1 패스(223a)는 64 바이트 블록 단위로 처리하며, 제2 패스(223b)는 64 바이트 블록들을 재조립한 단일의 PDU 단위로 데이터를 처리한다.

<65> 그리고, 제2 패스(223b)는 개인용 컴퓨터(240)로부터 수신하는 패킷 차단 규칙에 따라, 패턴 매칭 과정을 통해 제1 네트워크(110, 또는 제2 네트워크)로 수신된 패킷을 제2 네트워크(120, 또는 제1 네트워크)로 전달할 것인지 또는 폐기할 것인지 결정한다.

<66> 이러한 제2 패스(223b)의 결정 사항에 따라, 트래픽 매니저(224)는 수신한 PDU를 폐기하거나 또는 PL3 브리지 FPGA 칩(222)을 통해 라인 인터페이스부(210)로 전달한다.

<67> 이와 동시에, 제2 패스(223b)는 개인용 컴퓨터(240)로부터 수신하는 센싱 규칙에 따라, 패턴 매칭 과정을 통해 수신된 패킷을 제2 네트워크 프로세서부(230)로 전달할 것이지를 결정한다. 즉, 제2 패스(223b)는 수신한 패킷 중 일부 패킷을 제2 네트워크 프로세서부(230)로 통과시켜, 통과시킨 패킷의 페이로드를 검색하도록 한다.

<68> 이후, 제2 패스(223b)가 해당 PDU와 센싱 여부를 트래픽 매니저(224)로 전달하면 트래픽 매니저(224) 내의 멀티캐스터(224a)는 센싱할 PDU의 복사본(-복사 PDU-)을 만들고, 패킷 변환 엔진(224b)은 복사 PUD에 2바이트 정보를 추가하여 PL3 브리지 FPGA 칩(222)을 통해 제2 네트워크 프로세서부(230)로 전달한다.

<69> 이때, 멀티캐스터(224a)가 센싱한 패킷에 대해 복사 PDU를 별도로 더 만드는 이유는, 원래의 PDU는 상대 네트워크(목적지 네트워크)로 전달시키기 위함이다.

<70> 다음으로, 제2 네트워크 프로세서부(230)는 수신한 복사 PDU에 대해 스노트사에서 제공하는 룰(Rule)을 이용하여 네트워크 침입 여부를 검출하는데, 이러한 스노트 룰에 대한 표시예가 아래의 [표 2]이다.

<71> [표 2]

<72> #----------

<73> # X11 RULES(예 1)

<74> #----------

<75> alert tcp $EXTERNAL_NET any -> $HOME_NET 6000 (msg:"X11 MITcookie"; flags: A+ content: "MIT-MAGIC-COOKIE-1"; reference:arachnids,396; classtype:bad-unknown; sid:1225; rev:1;)

<76> #----------

<77> # X11 RULES (example: RuleIDGroup)(예 2)

<78> #----------

<79> alert tcp $EXTERNAL_NET any -> $HOME_NET 6000 (msg:"X11 xopen"; flags: A+; content: "|6c00 0b00 0000 0000 0000 0000|"; reference:arachnids,395; classtype:unknown; sid:1226; rev:1;)

<80> #----------

<81> # X11 RULES (example: RuleIDSimple)(예 3)

<82> #----------

<83> alert tcp $EXTERNAL_NET 6000:6005 -> $HOME_NET any (msg:"X11 outgoing"; flags: SA;
reference:arachnids,126; classtype:unknown; sid:1227; rev:1;)

<84> #---------------------------------------

<85> # Subseven22 is a Trojan Horse (example: RuleIDNew)(예 4)

<86> #---------------------------------------

<87> alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any(msg:"BACKDOOR subseven 22";
flow:to_server,established; content:"|0d0a5b52504c5d3030320d0a|";
reference:arachnids,485; reference:url,www.hackfix.org/subseven/;
classtype:misc-activity; sid:103; rev:5;)

<88> [표 2]에 도시된 바와 같이, 스노트 룰은 헤드(밑줄)와 옵션(중간괄호) 영역을 포함하고 있으며, 상기한 예 1에서 알 수 있듯이 제1 네트워크 프로세서(221) 내 패스 2(223)에서 사용한 센싱 룰의 프로토콜은 TCP, 송신지 IP 주소와 송신지 포트 주소는 모든 값(임의의 값), 목적지 IP 주소는 자신의 네트워크 주소, 목적지 포트 주소는 6000, 그리고 TCP의 ACK 플래그는 1임을 알 수 있다.

<89> 여기서, 제2 네트워크 프로세서부(230)로 전달되는 PDU를 첨부한 도면을 통해 알아본다.

<90> 도 4는 본 발명의 실시예에 따라 제2 네트워크 프로세서부(220)로 전송하는 패킷 데이터의 구성을 도시한 도면이다.

<91> 제1 네트워크 프로세서(221)로 입력되는 입력 PDU(300)는 센싱 여부에 따라 라인 인터페이스부(210)로 전송되는 출력 PDU(301) 및, 제2 네트워크 프로세서부(230)로 전송되는 복사 PDU(303)가 PL3 브리지 FPGA(222)로 전달된다.

<92> 이때, 앞서 언급한 바와 같이 패킷 변환 엔진(224b)이 복사 PDU(303)에 추가하는 정보인 룰 아이디(302)는 센싱 룰에 1:1 대응하여 만들어지는데, 경우에 따라서는 하나의 센싱 룰에 여러 개의 시그너쳐가 포함될 수도 있다.

<93> 즉, [표 2]의 스노트 룰 예에서 (예 1) 및 (예 2) 룰은 동일한 센싱 룰을 갖는데, 이는 하나의 룰 아이디에 대해 서로 다른 두 개의 시그너쳐가 존재하게 된다. 이러한 [표 2]의 스노트 룰에 근거하여 생성되는 룰 아이디는 아래의 [표 3]과 같다.

<94> [표 3]

<95>

| 룰 아이디 | 공격 종류 |
|---|---|
| 0x0001 | X11_MITcookie, X11_open |
| 0x0002 | X11_outgoing |
| 0x0003 | BACKDOOR_subseven22 |

<96> 도 5는 도 2에 도시한 PL3 브리지 FPGA 칩의 구성을 세부적으로 도시한 도면이다.

<97> 도 5에 도시되어 있듯이, PL3 브리지 FPGA 칩(222)은 제1 내지 제4 논리 포트(222a~222d)와 링크 레이이어 리시버(222e, 222f), PDU 변환/복사부(222g, 222h) 및 PHY 트랜스미터(222i, 222j)를 포함한다.

<98> 자세히 설명하면, 먼저 제1 논리포트(222a, 또는 제2 논리포트2)는 외부의 기가비트 이더넷 인터페이스(101, 또는 102)로 빠져나갈 출력 PDU(301)를 POS-PHY 레벨 3 인터페이스(202)를 통해 기가비트 PHY 칩(213)으로 전달한다.

<99> 그리고, 제3 논리포트(222c, 또는 제4 논리포트)는 기가비트 이더넷 포트(211, 또는 제2 기가비트 이더넷 포트)로부터 수신하는 복사 PDU(303)를 링크레이어 리시버(222e, 222f)로 전달한다.

<100> 이후, 링크레이어 리시버(222e, 222f)는 수신한 복사 PDU(303)를 PDU 변환/복사부(222g, 222h)로 전달하며, PDU 변환/복사부(222g, 222h)는 전달받은 복사 PDU를 이용하여 BPDU(Bearer PDU, 이하 'BPDU' 라 함)와 SPDU(Shortened PDU, 이하 'SPDU' 라 함)를 생성하여 PHY 트랜스미터(222i, 222j)로 전달한다.

<101> 이처럼, PDU 변환/복사부(222g, 222h)가 복사 PDU에 기초하여 BPDU와 SPDU를 모두 생성하는 이유는 추후에 이루어질 제2 네트워크 프로세서부(230)의 패턴 매칭시 실시간 매칭을 통한 빠른 대응을 수행하기 위함이다.

<102> 이후, PHY 트랜스미터(222i, 222j)는 생성한 BPDU와 SPDU를 POS-PHY 레벨 3 인터페이스(203)를 통해 제2 네트워크 프로세서부(230)로 전달한다.

<103> 여기서, PDU 변환/복사부(222g, 222h)가 생성하는 BPDU와 SPDU의 생성 과정을 도 4를 참조하여 알아본다.

<104> 먼저, PL3 브리지 FPGA 칩(222) 내의 PDU 변환/복사부(222g, 222h)는 수신한 복사 PDU(303)를 변환하여 제2 네트워크 프로세서부(230)에서의 시그너쳐 매칭에 불필요한 PDU 영역(306, 예를 들어 PDU 내의 헤드 등)을 제거한 BPDU(304)를 생성한 후, POS-PHY 레벨 3 인터페이스(203)를 통해 제2 네트워크 프로세서부(230)로 전달한다.

<105> 그리고, PDU 변환/복사부(222g, 222h)는 복사 기능을 이용해 생성한 BPDU(304) 보다 32 바이트(307) 줄어든 SPDU(305)를 생성한 후, POS-PHY 레벨 3 인터페이스(203)를 통해 제2 네트워크 프로세서부(230)로 전달한다.

<106> 도 6은 도 2에 도시한 제2 네트워크 프로세서의 구성을 세부적으로 도시한 도면이다.

<107> 도 6에 도시되어 있듯이, 제2 네트워크 프로세서(231)는 분류기(232)와 스테이트 엔진(233) 및 PCI 인터페이스(234)를 포함하며, 분류기(232)는 제1 패스(232a)를 포함한다.

<108> 분류기(232)는 스노트 룰에 근거한 패턴 매칭을 통해 네트워크 침입 여부 또는 공격을 검출하며, 스테이트 엔진(233)은 검출한 침입 또는 공격과 관련한 정보를 수집하여 관리한다. 그리고, PCI 인터페이스(234)는 PCI 버스(204)를 통해 검출한 침입 또는 공격 관련 정보를 개인용 컴퓨터(240)로 전송한다.

<109> 자세히 설명하면, 분류기(232)가 네트워크 침입 또는 공격을 검출하여 경보 메시지를 개인용 컴퓨터(240)로 전달하며, 개인용 컴퓨터(240)는 제3 패스(232a)로 새로운 스노트 룰을 전달한다. 그리고, 개인용 컴퓨터(240)는 검출된 공격을 차단하기 위해 제1 네트워크 프로세서부(220)로 트래픽 차단 규칙을 전달함으로서, 제1 또는 제2 네트워크를 실시간으로 보호한다.

<110> 즉, 분류기(232) 내의 제3 패스(232a)는 BPDU(304)와 SPDU(305)의 페이로드를 개인용 컴퓨터(240)로부터 수신하는 스노트 룰에 따라 패턴 매칭을 수행하여 공격 여부를 확인하는데, 이는 곧 BPDU(304)와 SPDU(305) 각각에 공격 시스너처가 존재하는지를 검사하는 것이다. 이러한 동작 과정을 첨부한 도면을 통해 설명한다.

<111> 도 7은 도 2에 도시한 제2 네트워크 프로세서부의 동작 과정을 순차적으로 도시한 흐름도이다.

<112> 도 7에 도시되어 있듯이, 먼저 제3 패스(232a)는 제1 네트워크 프로세서부(220)로부터 수신(S710)하는 BPDU(304)와 SPDU(305)를 64바이트 크기의 블록 단위로 나누어서 처리한다.

<113> 이처럼, 제3 패스(232a)가 64바이트 크기로 패킷 데이터를 나누어서 처리하는 이유는 제3 패스(232a)가 내장되어 있는 제2 네트워크 프로세서(231)인 APP500이 그 특성상 64바이트로 데이터를 처리하기 때문이다.

<114> 자세히 설명하면, 제3 패스(232a)는 BPDU(304)와 SPDU(305)의 길이가 64바이트 이하이면 싱글 블록으로, 65바이트 이상이나 128바이트 이하이면 단일의 시작 블록과 단일의 마지막 블록으로 구성한다.

<115> 반면, BPDU(304)와 SPDU(305)의 총 데이터 크기가 129바이트 이상이면, 제3 패스(232a)는 단일의 시작 블록과 여러 개의 중간 블록, 그리고 단일의 마지막 블록으로 구성한다.

<116> 먼저, 제3 패스(232a)는 제1 네트워크 프로세서부(220)로부터 수신하는 블록이 싱글 블록인지 또는 시작 블록인지를 확인(S720)한 후, 확인 결과 싱글 블록이거나 시작 블록이면 수신한 첫 블록에 룰 아이디(2바이트 정도)가 있는지를 확인한다(S730).

<117> 확인 결과, 룰 아이디가 존재하면 제3 패스(232a)는 블록이 싱글 블록인지를 확인(S740)한 후, 싱글 블록이면 그에 따른 처리 루틴을 수행한다(S780).

<118> 반면, 블록이 싱글 블록이 아닌 시작 블록이면, 제3 패스(232a)는 해당 PDU의 중간 블록 또는 마지막 블록이 계속해서 들어올 것을 예상하여 시작 블록의 룰 아이디를 글로벌 레지스터(global register, 미도시)에 저장(S750)한 후, 시작 또는 중간 블록의 처리 루틴을 수행한다(S790).

<119> 한편, 첫 번째 블록이 룰 아이디가 존재하지 않으면, 제3 패스(232a)는 에러 처리(S810)를 수행한다.

<120> 이후, 제3 패스(232a)는 블록이 중간 또는 마지막 블록이면, 해당 블록의 룰 아이디가 글로벌 레지스터가 존재 하는지 확인(S760)한 후, 확인 결과 존재하지 않으면 에러 처리를 수행한다(S820).

<121> 반면, 해당 블록의 룰 아이디가 존재하면, 제3 패스(232a)는 해당 블록이 마지막 블록인지 검사(S770)한 후, 마지막 블록이면 마지막 블록 처리 루틴(S800)을 수행하고, 중간 블록이면 시작 또는 중간 블록 처리 루틴(S780)에 따라 수행한다.

<122> 그러면, 각 블록별(싱글, 시작, 중간 및 마지막 블록) 처리 루틴을 첨부한 도면을 통해 알아본다.

<123> 도 8은 도 7에 도시한 싱글 블록 처리 과정을 순차적으로 도시한 흐름도이다.

<124> 제3 패스(232a)는 싱글 블록에 대한 패턴 매칭을 수행하기 위해, 도 8에 도시되어 있듯이 먼저 $currOffset + Lmin > 63($currLength)을 확인한다(S781).

<125> 이때, $currOffset은 현 블록의 패턴 검사를 위한 시작 포인터이며, Lmin은 현 룰 아이디에 속해 있는 시그너쳐들 중 길이가 가장 짧은 시그너쳐의 길이, $currLength는 현 블록의 총 길이를 의미한다.

<126> 이후, 확인 결과 '예' 이면, 제3 패스(232a)는 싱글 블록에 대한 패턴 매칭 과정을 종료(S900)하는 반면, 확인 결과 '아니오' 이면, 제3 패스(232a)는 패턴 매칭을 수행한다(S782).

<127> 이때, 패턴 매칭 결과 공격 시그너쳐가 발견(S783)되면, 제3 패스(232a)는 개인용 컴퓨터(240)로 경보를 발생(S784)한 후, 동작 과정을 종료한다(S900).

<128> 한편, 제3 패스(232a)는 패턴 매칭 결과 공격 시그너쳐가 발견되는 않았으면, $currLength < 32 인지를 검사한다(S785).

<129> 이때, $currLength는 현 블록의 총 길이로서, 최소 0에서 최대 63 바이트까지의 값을 가질 수 있다. 그리고, 32바이트를 최대 한계로 하여 검사하는 이유는 앞서 언급한 바와 같이, 네트워크로 입력된 PDU가 BPDU(304)와 SPDU(305)로 만들어져 네트워크로부터 입력된 PDU를 구성하는 각 64 바이트 블록의 처음 32바이트는 BPDU에서 해당 시그너쳐를 검색하고, 나머지 32바이트는 SPDU에서 해당 시그너쳐를 검색하기 때문에, 패턴 매칭을 통해 검사할 바이트는 최대 32바이트로 제한하는 것이다. 즉, 그 이상의 데이터 바이트는 패턴 매칭시 불필요한 데이터로서, 오히려 실시간 장애 검출에 방해가 된다.

<130> 검사 결과, $currLength < 32이 '아니오'이면 제3 패스(232a)는 싱글 블록에 대한 지금까지의 패턴 매칭 횟수가 32번째인지 확인(S786)하는 반면, "예"이면, 동작 과정을 종료한다.

<131> 한편, 제3 패스(232a)는 $currLength < 32가 '예'이거나 싱글 블록에 대한 패턴 매칭 횟수가 32 번째가 아니면, 패턴 매칭 시작 포인터 이동 수단(이하 'fRSkip()' 이라 함)을 이용한 $currOffset 조정(S787)한 후, 다시 $currOffset + Lmin > 63(S787)을 확인한다.

<132> 이와 같은 공격 시그너쳐 검출 과정 중의 하나인 싱글 블록 생성 과정을 도 9를 통해 개념적으로 설명하면 다음과 같다.

<133> 도 9는 본 발명의 실시예에 따른 싱글 블록 생성 과정을 개념적으로 도시한 도면이다.

<134> 도 9에 도시된 바와 같이, 복사 PDU(303)에서 룰 아이디(302)와 패턴 매칭에서 제외될 영역(306, 예를 들어 헤드 영역)을 제외한 크기가 32바이트 이하이면, 제3 패스(232a)는 싱글 블록으로 구성된 하나의 BPDU(600)만을 생성한다.

<135> 반면, 복사 PDU(303)가 룰 아이디(302)와 패턴 매칭에서 제외될 영역(306)을 제외하고 32바이트 이상이거나 62바이트 이하이면, 제3 패스(232a)는 싱글 블록으로 구성된 하나의 BPDU(601)와 싱글 블록으로 구성된 하나의 SPDU(602)를 생성한다.

<136> 또한, 복사 PDU(303)가 룰 아이디(302)와 패턴 매칭에서 제외될 영역(306)을 제외하고 62바이트 이상이거나 94바이트 이하이면, 제3 패스(232a)는 시작 블록(605)과 마지막 블록(606)으로 구성된 하나의 BPDU(603)와 싱글 블록으로 구성된 하나의 SPDU(604)를 생성한다.

<137> 다음으로, 시작 또는 중간 블록 처리 루틴에 대해 알아보면, 도 10은 도 7에 도시한 시작 또는 중간 블록 처리 과정을 순차적으로 도시한 흐름도이다.

<138> 도 10에 도시되어 있듯이, 제3 패스(232a)는 제1 네트워크 프로세서부(230)로부터 수신한 블록이 '시작블록&PDU=SPDU?' 인지를 검사(791)하여, 검사 결과 맞으면, 즉 시작 블록이면서 SPDU이면, 제3 패스(232a)는 $currOffset=33인지를 검사한다(S792).

<139> 반면, 수신한 블록이 시작 블록도 아니며 SPDU도 아니라면, 제3 패스(232a)는 $currOffset=35?인지를 검사한다(S793).

<140> 이때, 상기한 두 조건(S792, S793)이 맞으면, 현재의 블록에는 해당 시그너처가 없음을 의미하고, 따라서 공격 검출 과정을 종료(S900)하는 반면, 상기한 두 조건을 모두 만족하지 않으면, 제3 패스(232a)는 개인용 컴퓨터(240)로부터 수신하는 스노트 룰(공격 시그너처)에 따라 패턴 매칭을 수행한다(S794).

<141> 이때, 공격 시그너처와 매칭되는 패턴을 발견하면, 제3 패스(232a)는 개인용 컴퓨터(240)로 경보 발생(S795)을 수행하는 반면, 공격 시그너처와 동일한 패턴이 발견되지 않으면,

제3 패스(232a)는 fRSkip()을 이용하여 $currOffset 조정(S796)을 수행한 후, 다시 시작블록&PDU=SPDU?를 검사하게 된다.

<142> 여기서, 시작 블록 또는 중간 블록이 만들어지는 과정을 첨부한 도면을 통해 설명하면, 도 11은 본 발명의 실시예에 따른 시작 블록 또는 중간 블록 생성 과정을 개념적으로 도시한 도면이다.

<143> 도 11에 도시된 바와 같이, 복사 PDU(303)에서 룰 아이디(302)와 패턴 매칭에서 제외할 영역(306)을 제외한 데이터 크기가 126바이트 이상이거나 158바이트 이하이면, 제3 패스(232a)는 시작 블록(608), 중간 블록(609), 그리고 32 바이트 보다 작은 마지막 블록으로 구성된 하나의 BPDU(607)를 생성한다.

<144> 그리고, 제3 패스(232a)는 시작 블록(612)과 32바이트 이하인 마지막 블록(613)으로 구성된 하나의 SPDU(611)를 생성한다.

<145> 또한, 제3 패스(232a)는 복사 PDU(303)에서 룰 아이디(302)와 패턴 매칭에서 제외할 영역(306)을 제외한 데이터 크기가 158바이트 이상이거나 190바이트 이하이면, 시작 블록(614), 중간 블록(615), 그리고 32바이트 이상인 마지막 블록(616)으로 구성된 BPDU(617)을 생성한다.

<146> 그리고, 제3 패스(232a)는 시작 블록(619), 중간 블록(620) 및 32바이트 이하인 마지막 블록(621)으로 구성된 하나의 SPDU(618)를 생성한다.

<147> 다음으로, 마지막 블록 처리 루틴에 대해 첨부한 도면을 참조하면, 도 12는 도 7에 도시한 마지막 블록 처리 과정을 순차적으로 도시한 흐름도이다.

<148> 도 12에 도시되어 있듯이, 먼저 제3 패스(232a)는 $currOffset + Lmin > 63인지를 확인(S810)한 후, 확인 결과 맞으면 공격 여부 검출 과정을 종료(S900)하는 반면, 확인 결과 맞지 않으면 제3 패스(232a)는 개인용 컴퓨터(240)로부터 수신하는 스노트 룰(공격 시그너쳐)에 따라 패턴 매칭을 수행한다(S820).

<149> 이때, 개인용 컴퓨터(240)로부터 수신하는 공격 시그너쳐는 관리자에 의해 또는 실시간으로 변화하는 공격 유형에 따라 변화하는 것으로서, 그 특성상 가변적인 것이다.

<150> 이후, 패턴 매칭 수행 결과, 기준이 되는 공격 시그너쳐와 일치하는 패턴이 발생하면, 제3 패스(232a)는 개인용 컴퓨터(240)로 경보를 발생(S850)하는 반면, 일치하는 패턴이 발생하는 발생하면, 제3 패스(232a)는 $currLength < 32(S830)를 확인한다. 이때, $currLength는 현 블록의 총 길이를 나타내며 0에서 63까지 범위의 값을 가질 수 있다.

<151> 이후, $currLength < 32의 조건을 만족하지 않는 것으로 확인되면, 제3 패스(232a)는 지금까지 현 블록에 대한 패턴 매칭 횟수가 32 번째인지 검사(S840)한 후, 상기한 조건을 만족하면 공격 여부 검출 과정을 종료한다(S900).

<152> 반면, 상기한 조건을 만족하지 않으면, 제3 패스(232a)는 fRSkip()을 이용하여 $currOffset를 조정(S860)한 후, 다시 $currOffset + Lmin > 63(S810)를 수행한다.

<153> 이처럼, 본 발명의 실시예에 따른 인-라인 모드 네트워크 검출/차단 장치 및 그 방법은 네트워크를 통해 송수신하는 패킷을 모니터링하여 다양한 통계 자료 수집과 함께 차단 규칙에 의거한 패킷 필터링 및, 센싱을 수행하는 제1 네트워크 프로세서부와, 알려진 공격 시그너쳐를 기준으로 패킷의 페이로드를 조사하여 네트워크 침입 여부 또는 공격 산출을 검출한 후, 이를 차단하는 제2 네트워크 프로세서부를 포함한다.

<154> 즉, 본 발명은 네트워크로의 침입 여부 확인 및 그에 따른 공격 차단을 기가비트 이더넷 포트를 수용하여 실시간으로 처리함으로써, 네트워크 침입에 대한 빠른 대응을 할 수 있을 뿐만 아니라, 기가비트급의 대용량 트래픽을 안정적으로 처리할 수 있다.

<155> 도면과 발명의 상세한 설명은 단지 본 발명의 예시적인 것으로서, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

【발명의 효과】

<156> 본 발명에 따른 인-라인 모드 네트워크 검출/차단 장치 및 그 방법은 네트워크로의 침입 여부 확인 및 그에 따른 공격 차단을 기가비트 이더넷 포트를 수용하여 실시간으로 처리함으로써, 네트워크 침입에 대한 빠른 대응을 할 수 있을 뿐만 아니라, 기가비트급의 대용량 트래픽을 안정적으로 처리할 수 있다.

<157> 또한, 본 발명은 트래픽을 미터링하는 규칙에서부터 필터링 규칙 및 센싱 규칙에 이르기까지 공격 여부를 검출 및 차단하는데 필요한 각종 기준들을 관리자(개인용 컴퓨터)를 통해 실시간으로 업데이트할 수 있을 뿐만 아니라, 이를 통한 사용의 편리성 및 경제적 이점을 누릴 수 있는 효과가 있다.

<158> 또한, 본 발명은 패킷 데이터를 포워딩(forwarding)하는 과정과 패킷 데이터의 페이로드를 검색하는 과정을 각각 분리하여 운영함으로서, 인-라인 모드 시스템의 안정성을 높일 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

보호 네트워크와 외부 네트워크 사이에 연결되며, 상기 보호 네트워크와 상기 외부 네트워크 간의 침입 여부를 탐지하여 차단하는 시스템에 있어서,

외부로부터 수신하는 PDU(Packet Data Unit)를 모니터링하여 미터링 규칙에 따라 각종 통계치 자료를 수집하며, 상기 수신한 PDU를 패킷 차단 규칙에 따라 선택적으로 폐기하거나 통과시키고, 센싱 규칙에 따라 상기 수신한 PDU를 복사한 복사 PDU를 만드는 제1 네트워크 프로세서부;

상기 제1 네트워크 프로세서부로부터 수신하는 PDU의 페이로드(payload)에 대해 적어도 한 개 이상의 공격 시그너쳐를 이용하여 상기 보호 및 외부 네트워크간의 침입 여부를 탐지하는 제2 네트워크 프로세서부; 및

상기 제2 네트워크 프로세서부에서 탐지한 침입을 차단할 수 있는 규칙인 패킷 차단 규칙을 생성하거나 갱신하여 상기 제1 네트워크 프로세서부로 제공하는 개인용 컴퓨터

를 포함하는 인-라인 모드 네트워크 침입 탐지/차단 시스템.

【청구항 2】

제1 항에 있어서,

외부의 기가비트 이더넷 인터페이스(Gigabit Ethernet Interface)로부터 수신하는 적어도 한 개 이상의 PDU를 상기 제1 네트워크 프로세서부로 전달하는 라인 인터페이스부

를 더 포함하는 인-라인 모드 네트워크 침입 탐지/차단 시스템.

【청구항 3】

제2 항에 있어서,

상기 개인용 컴퓨터는,

상기 PDU의 송신지 및 목적지 포트 주소, 송신지 IP(Internet Protocol) 주소와 목적지 IP 주소, 프로토콜 및 TCP(Transmission Control Protocol) 플래그 비트 중 적어도 하나 이상을 포함하거나, 또는 두 개 이상의 조합으로 구성되는 패킷 차단 규칙과 센싱 규칙을 생성하거나 업데이트하는 것을 특징으로 하는 인-라인 모드 네트워크 침입 탐지/차단 시스템.

【청구항 4】

제3 항에 있어서,

상기 개인용 컴퓨터는,

상기 PDU의 송신지 및 목적지 이더넷 주소와 이더넷 타입, 송신지 IP 주소, 목적지 IP 주소, 송신지 포트 주소, 목적지 포트 주소, 프로토콜, TCP 플래그 비트 중 적어도 하나 이상을 포함하거나, 또는 두 개 이상의 조합으로 구성되는 미터링 규칙을 생성하거나 업데이트하는 것을 특징으로 하는 인-라인 모드 네트워크 침입 탐지/차단 시스템.

【청구항 5】

제4 항에 있어서,

상기 제1 네트워크 프로세서부는,

상기 개인용 컴퓨터로부터 수신하는 패킷 차단 규칙에 따라 상기 라인 인터페이스부로부터 수신하는 PDU를 폐기할 것인지 또는 통과시킬 것인지를 결정하고, 상기 개인용 컴퓨터로부터 수신하는 센싱 규칙에 따라 상기 수신한 PDU를 복사할 것인지를 결정하는 분류기;

상기 분류기의 폐기 처리 결정에 따라, 상기 수신한 PDU를 폐기하거나 또는 센싱하기로 결정한 PDU를 복사하여 복사 PDU를 생성하는 트래픽 매니저; 및

상기 개인용 컴퓨터로부터 수신하는 트래픽 미터링 규칙에 따라, 상기 라인 인터페이스부로부터 수신하는 PDU와 관련 있는 각종 통계치 자료를 관리하는 스테이트 엔진

를 포함하는 인-라인 모드 네트워크 침입 탐지/차단 시스템.

【청구항 6】

제5 항에 있어서,

상기 제1 네트워크 프로세서부는,

상기 기가비트 이더넷 인터페이스로 PDU를 다시 빠져 나가게 하거나 상기 기가비트 이더넷 인터페이스로부터 PDU를 수신하는 제1 내지 제4 논리 포트;

상기 스테이트 엔진으로부터 출력되는 복사 PDU를 수신하는 링크레이어 리시버;

상기 수신한 복사 PDU를 이용하여 BPDU(Bearer PDU)와 SPDU(Shortened PDU)를 생성하는 PDU 변환/복사부; 및

상기 생성한 BPDU와 SPDU를 상기 제2 네트워크 프로세서부로 전송하는 PHY 트랜스미터

를 더 포함하는 인-라인 모드 네트워크 침입 탐지/차단 시스템.

【청구항 7】

제6 항에 있어서,

상기 제2 네트워크 프로세서부는,

상기 전송한 BPDU와 SPDU의 페이로드를 상기 개인용 컴퓨터로부터 수신하는 룰에 따라 패턴 매칭을 수행하여 상기 보호 및 외부 네트워크간의 침입 여부를 탐지하는 분류기;

상기 탐지한 침입 여부와 관련한 정보를 수집하여 관리하는 스테이트 엔진; 및

상기 수집하여 관리하는 정보를 상기 개인용 컴퓨터로 전송하는 PCI 인터페이스

를 포함하는 인-라인 모드 네트워크 침입 탐지/차단 시스템.

【청구항 8】

보호 네트워크와 외부 네트워크 사이에 연결되며, 상기 보호 네트워크와 상기 외부 네트워크 간의 침입 여부를 탐지하여 차단하는 방법에 있어서,

a) 외부로부터 수신하는 PDU(Packet Data Unit)를 적어도 한 개 이상 폐기시키거나 그대로 통과시킬 수 있는 기준인 패킷 차단 규칙을 생성하는 단계;

b)상기 생성한 패킷 차단 규칙에 따라 상기 수신하는 PDU를 선택적으로 폐기하거나 통과시키는 단계; 및

c)상기 통과시킨 PDU의 페이로드(payload)에 대해 적어도 한 개 이상의 공격 시그너쳐를 이용하여 상기 보호 및 외부 네트워크간의 침입 여부를 탐지하는 단계; 및

d) 상기 탐지한 침입을 차단할 수 있는 규칙을 생성하거나 업데이트하여 상기 탐지한 공격을 차단시키는 단계

를 포함하는 인-라인 모드 네트워크 침입 탐지/차단 방법.

【청구항 9】

제8 항에 있어서,

상기 a)단계는,

상기 수신한 PDU의 송신지와 목적지 포트 주소, 송신지 IP(Internet Protocol) 주소와 목적지 IP 주소, 프로토콜 및 TCP(Transmission Control Protocol) 플래그 비트 중 적어도 한 개 이상을 포함하거나 또는 두 개 이상의 조합으로 구성되는 패킷 차단 규칙을 생성하거나 업데이트하는 단계;

상기 수신한 PDU의 송신지 및 목적지 포트 주소와 송신지 IP(Internet Protocol) 주소와 목적지 IP 주소, 프로토콜 및 TCP(Transmission Control Protocol) 플래그 비트 중 적어도 한 개 이상을 포함하거나 또는 두 개 이상의 조합으로 구성되는 센싱 규칙을 생성하거나 업데이트하는 단계; 및

상기 수신한 PDU의 송신지 및 목적지 이더넷 주소와 이더넷 타입, 송신지 IP 주소, 목적지 IP 주소, 송신지 포트 주소, 목적지 포트 주소, 프로토콜, TCP 플래그 비트 중 적어도 한 개 이상을 포함하거나 또는 두 개 이상의 조합으로 구성되는 미터링 규칙을 생성하거나 업데이트하는 단계

를 포함하는 인-라인 모드 네트워크 침입 탐지/차단 방법.

【청구항 10】

제9 항에 있어서,

상기 b)단계는,

상기 생성하거나 갱신한 패킷 차단 규칙에 따라, 상기 외부로부터 수신하는 PDU를 폐기 처리할 것인지 또는 통과시킬 것인지를 결정하는 단계;

상기 수신한 PDU 중 적어도 한 개 이상의 PDU를 폐기 처리하기로 결정하였으면, 상기 수신한 PDU를 폐기 처리하는 단계;

상기 수신한 PDU 중 적어도 한 개 이상의 PDU를 통과시키기로 결정하였으면, 상기 통과시키기로 결정한 PDU를 복사하여 복사 PDU를 생성하는 단계; 및

상기 생성한 복사 PDU에 추가 정보인 아이디(ID)를 포함시켜 출력시키는 단계

를 포함하는 인-라인 모드 네트워크 침입 탐지/차단 방법.

【청구항 11】

제10 항에 있어서,

상기 b)단계는,

상기 출력시키는 복사 PDU를 이용하여 BPDU(Bearer PDU)를 생성하는 단계; 및

상기 생성한 BPDU 보다는 작은 크기를 가진 SPDU(Shortened PDU)를 생성하여 상기 BPDU와 함께 출력시키는 단계

를 더 포함하는 인-라인 모드 네트워크 침입 탐지/차단 방법.

【청구항 12】

제11 항에 있어서,

상기 c)단계는,

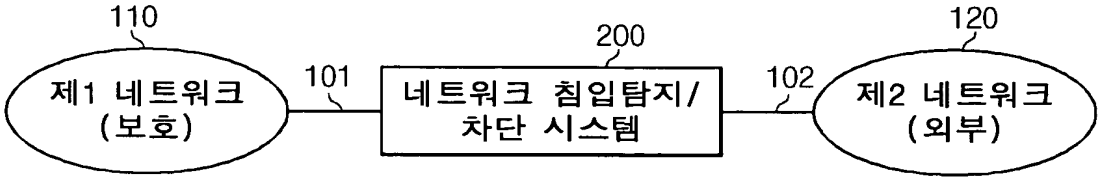
상기 출력시킨 BPDU 및 SPDU의 페이로드(payload)를 상기 보호 또는 외부 네트워크를 관리하는 관리자가 제시하는 공격 시그너쳐와 비교하는 패턴 매칭을 수행하는 단계; 및

상기 수행한 패턴 매칭 결과에 따라 상기 보호 또는 외부 네트워크로의 공격 여부를 감지한 후, 상기 감지한 결과를 상기 관리자에게 전달하여 상기 관리자가 제시하는 공격 시그너쳐를 업데이트하거나 다시 생성하도록 하는 단계

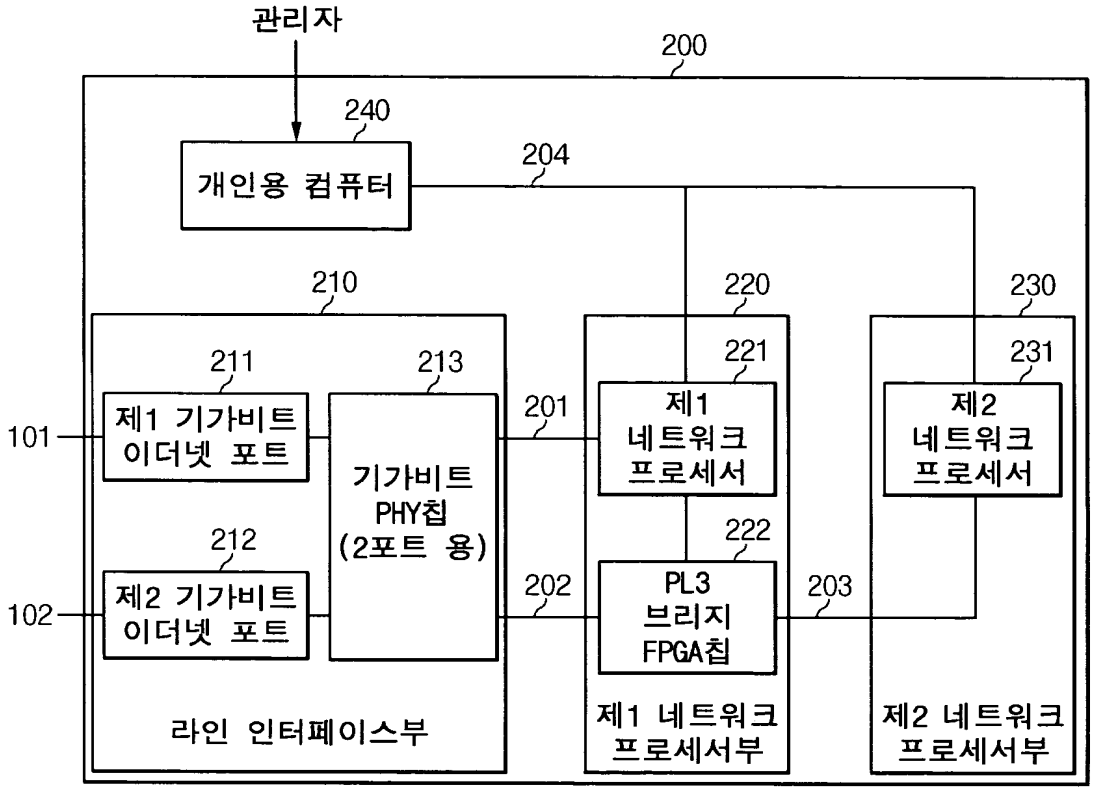
를 포함하는 인-라인 모드 네트워크 침입 탐지/차단 방법.

【도면】

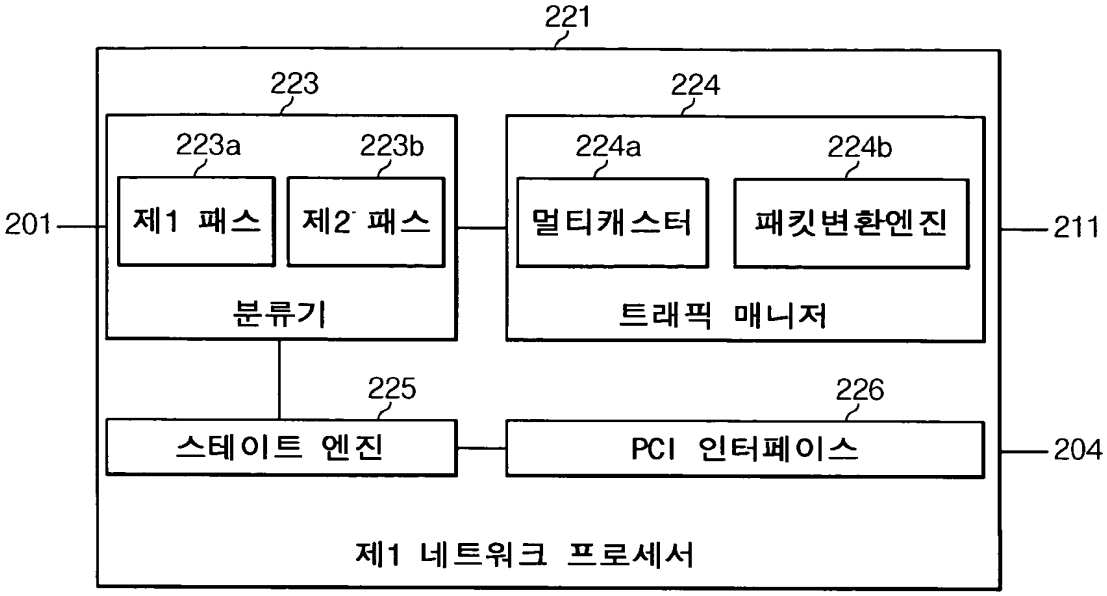
【도 1】


110
제1 네트워크
(보호)
101
200
네트워크 침입탐지/
차단 시스템
102
120
제2 네트워크
(외부)

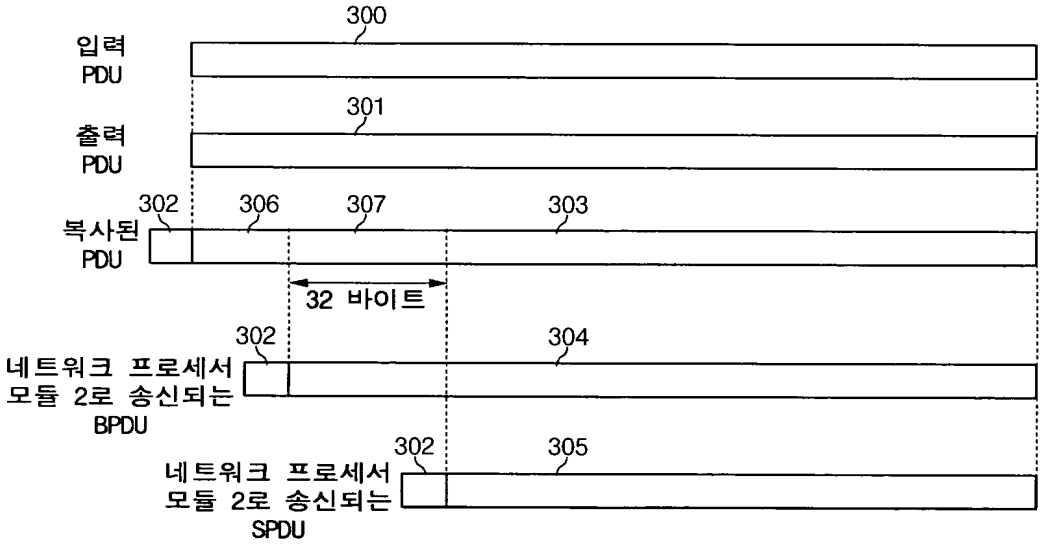
【도 2】


관리자
200
240
개인용 컴퓨터
204
210
211
제1 기가비트
이더넷 포트
213
기가비트
PHY칩
(2포트 용)
212
제2 기가비트
이더넷 포트
101
102
201
202
220
221
제1
네트워크
프로세서
222
PL3
브리지
FPGA칩
203
230
231
제2
네트워크
프로세서
라인 인터페이스부
제1 네트워크
프로세서부
제2 네트워크
프로세서부

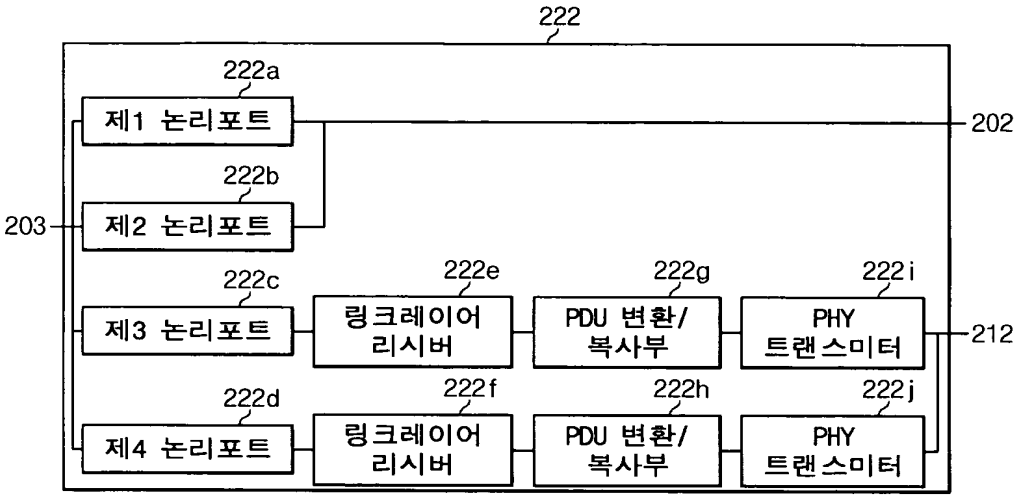
【도 3】


221
223
224
223a
223b
224a
224b
201
제1 패스
제2 패스
멀티캐스터
패킷변환엔진
211
분류기
트래픽 매니저
225
226
스테이트 엔진
PCI 인터페이스
204
제1 네트워크 프로세서

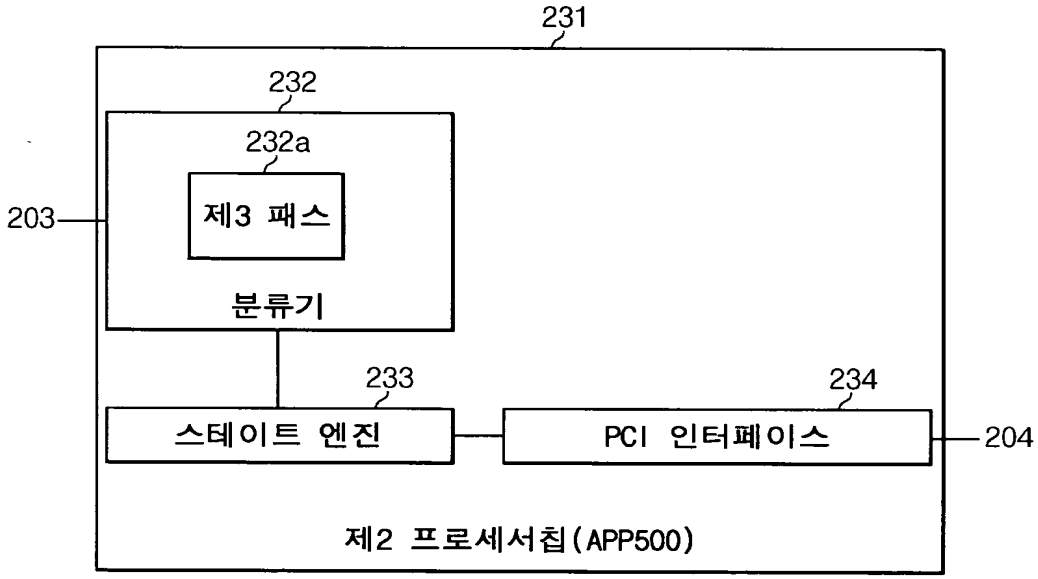
【도 4】


300
입력 PDU
301
출력 PDU
302
306
307
303
복사된 PDU
32 바이트
302
304
네트워크 프로세서 모듈 2로 송신되는 BPDU
302
305
네트워크 프로세서 모듈 2로 송신되는 SPDU

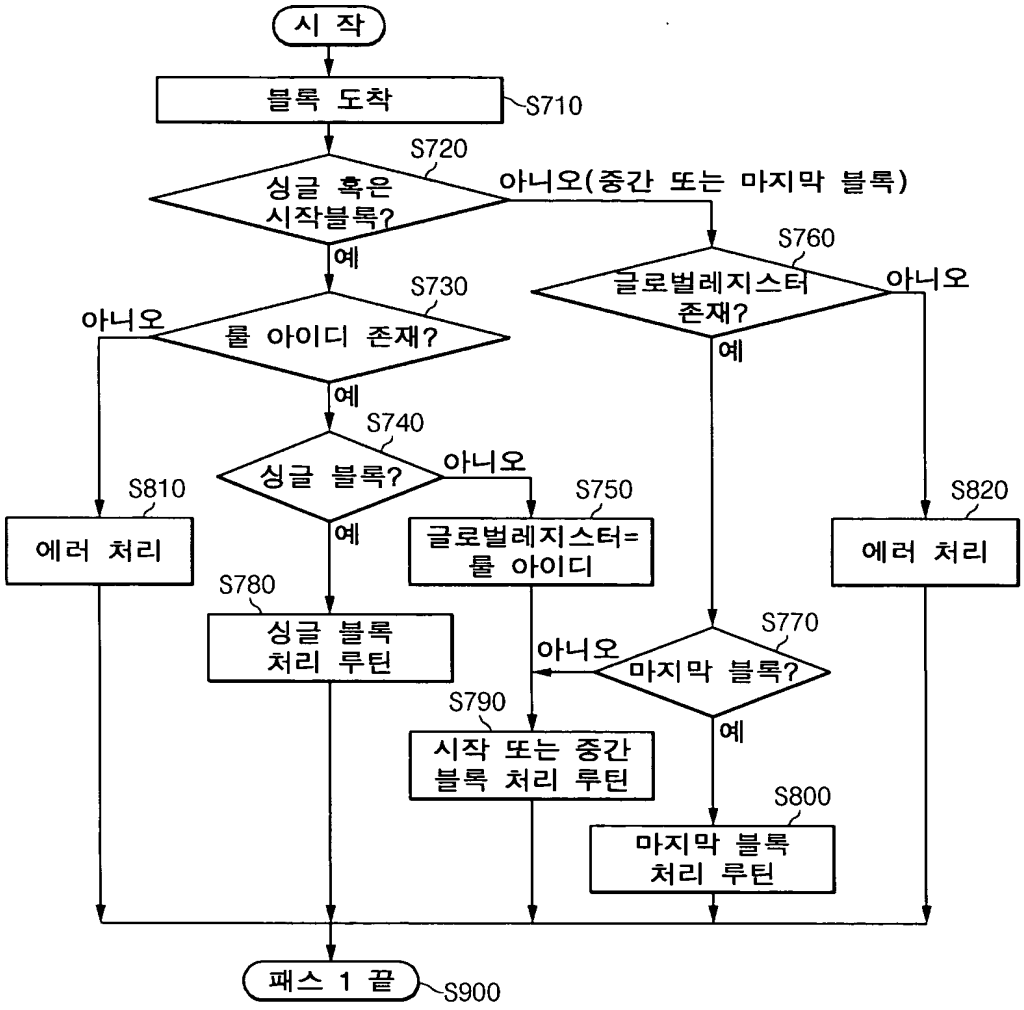
【도 5】


222
222a
제1 논리포트
202
222b
203
제2 논리포트
222c
222e
222g
222i
제3 논리포트
링크레이어 리시버
PDU 변환/ 복사부
PHY 트랜스미터
212
222d
222f
222h
222j
제4 논리포트
링크레이어 리시버
PDU 변환/ 복사부
PHY 트랜스미터

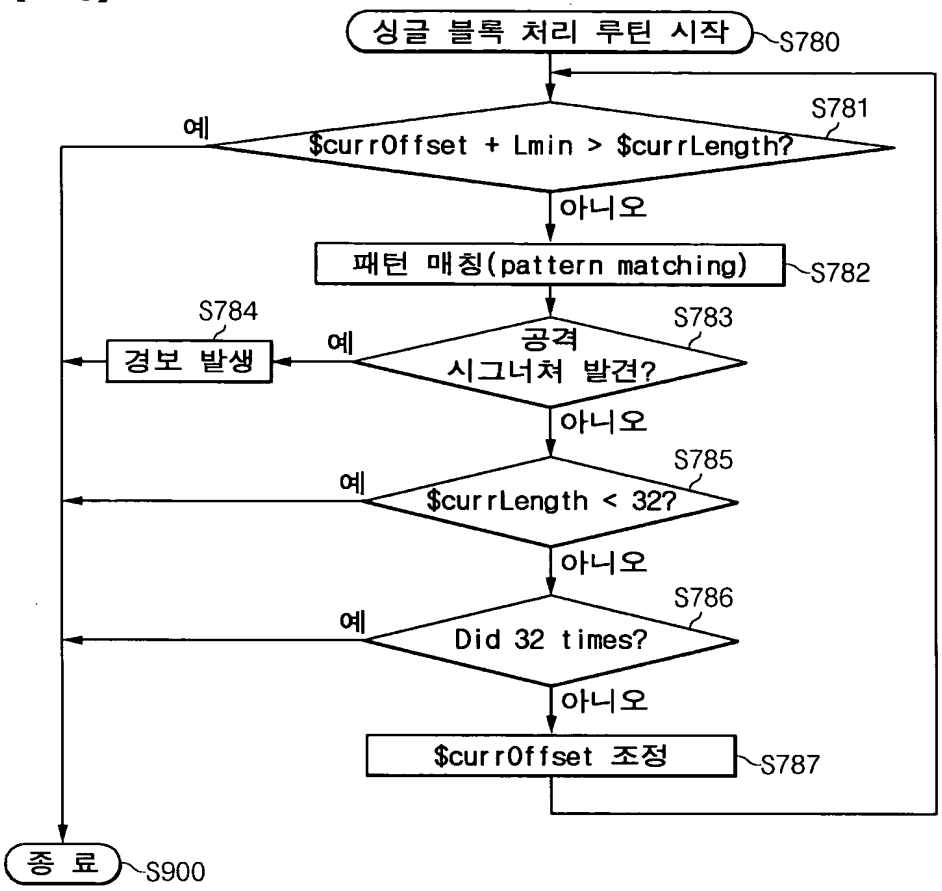
【도 6】


231
232
232a
203
제3 패스
분류기
233
234
스테이트 엔진
PCI 인터페이스
204
제2 프로세서칩(APP500)

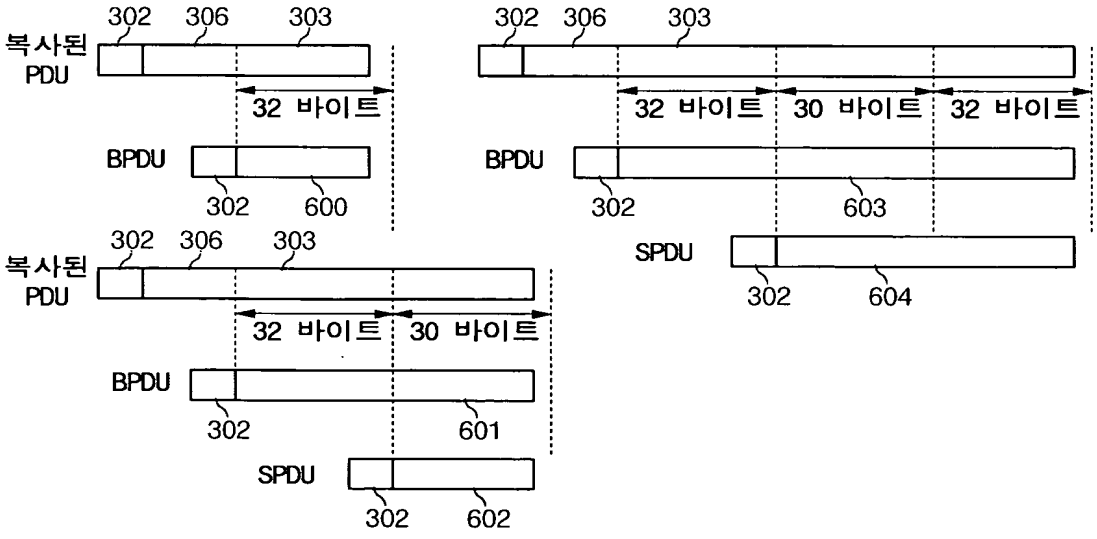
【도 7】


시 작
블록 도착
S710
S720
싱글 혹은 시작블록?
아니오(중간 또는 마지막 블록)
예
S730
룰 아이디 존재?
아니오
예
S740
싱글 블록?
아니오
예
S760
글로벌레지스터 존재?
아니오
예
S810
에러 처리
S750
글로벌레지스터= 룰 아이디
S820
에러 처리
S780
싱글 블록 처리 루틴
S770
마지막 블록?
아니오
예
S790
시작 또는 중간 블록 처리 루틴
S800
마지막 블록 처리 루틴
패스 1 끝
S900

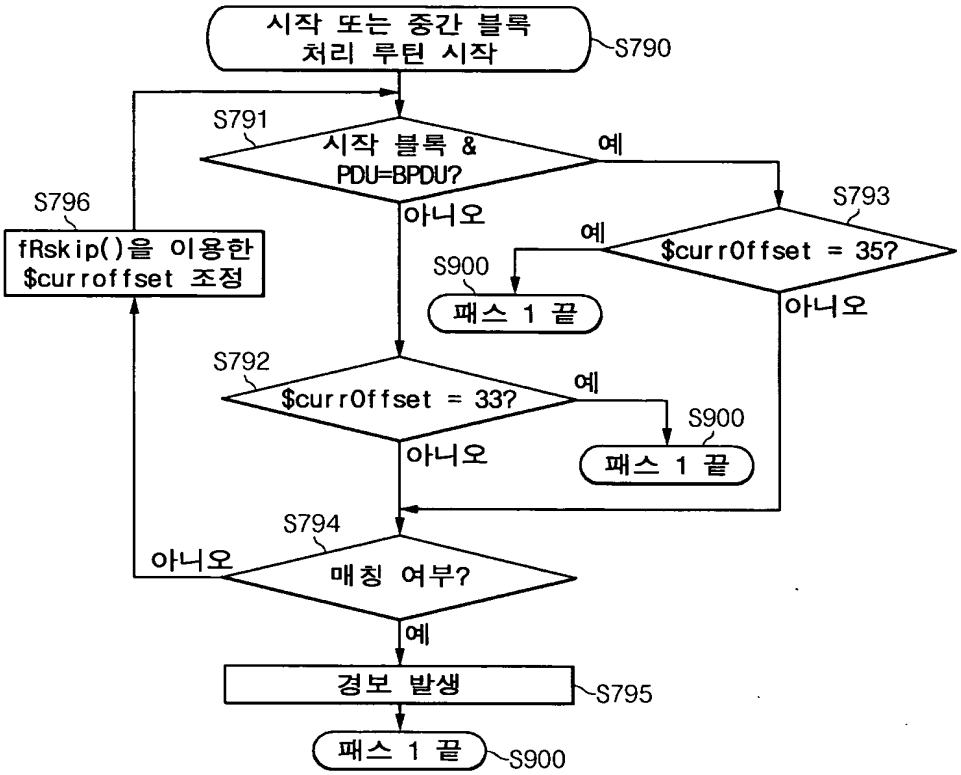
【도 8】


싱글 블록 처리 루틴 시작
S780
S781
예
$currOffset + Lmin > $currLength?
아니오
패턴 매칭(pattern matching)
S782
S784
S783
경보 발생
예
공격 시그너쳐 발견?
아니오
S785
예
$currLength < 32?
아니오
S786
예
Did 32 times?
아니오
$currOffset 조정
S787
종 료
S900

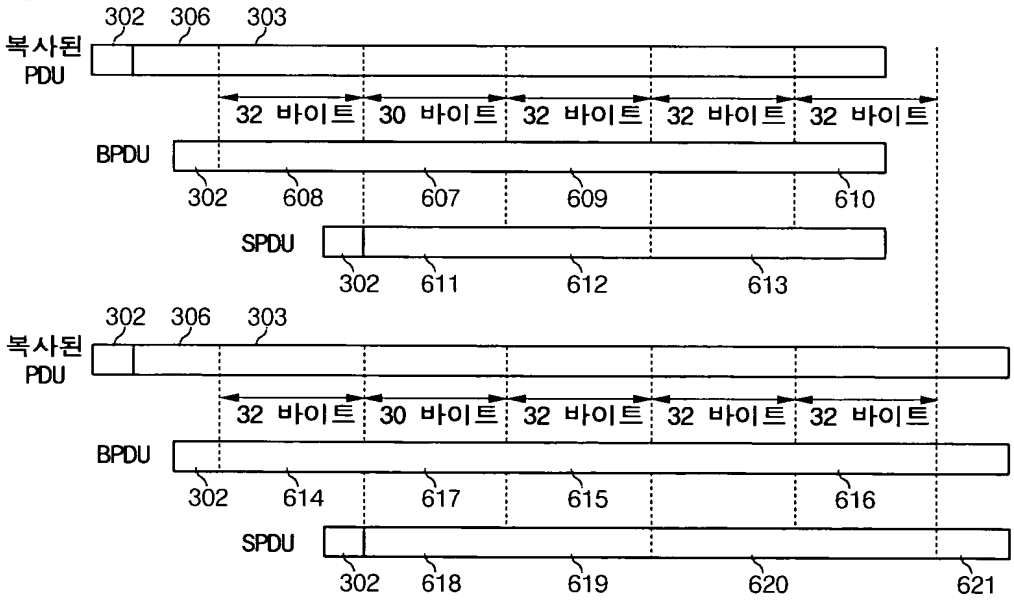
【도 9】


302
306
303
복사된 PDU
32 바이트
BPDU
302
600
302
306
303
32 바이트
30 바이트
32 바이트
BPDU
302
603
SPDU
302
604
302
306
303
복사된 PDU
32 바이트
30 바이트
BPDU
302
601
SPDU
302
602

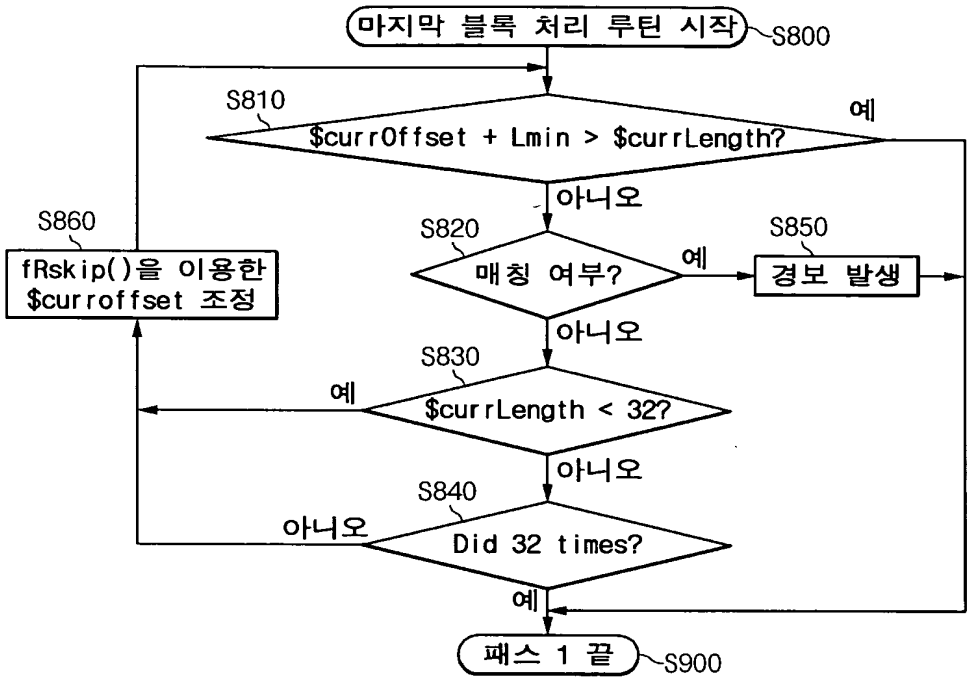
【도 10】


시작 또는 중간 블록 처리 루틴 시작
S790
S791
시작 블록 & PDU=BPDU?
예
아니오
S793
$curr0ffset = 35?
예
아니오
S900
패스 1 끝
S796
fRskip()을 이용한 $curroffset 조정
S792
$curr0ffset = 33?
예
아니오
S900
패스 1 끝
S794
매칭 여부?
아니오
예
경보 발생
S795
패스 1 끝
S900

【도 11】


302
306
303
복사된 PDU
32 바이트
30 바이트
32 바이트
32 바이트
32 바이트
BPDU
302
608
607
609
610
SPDU
302
611
612
613
302
306
303
복사된 PDU
32 바이트
30 바이트
32 바이트
32 바이트
32 바이트
BPDU
302
614
617
615
616
SPDU
302
618
619
620
621

【도 12】


마지막 블록 처리 루틴 시작
S800
S810
$currOffset + Lmin > $currLength?
예
아니오
S820
매칭 여부?
예
S850
경보 발생
아니오
S860
fRskip()을 이용한
$curroffset 조정
S830
$currLength < 32?
예
아니오
S840
Did 32 times?
아니오
예
패스 1 끝
S900